



$$\begin{array}{c}
 \left\{ \begin{array}{l}
 \text{IS} \\
 \begin{array}{c}
 \xrightarrow{X \cdot g \cdot n} \quad \xrightarrow{X = g^x \bmod n} \\
 \xrightarrow{Y = g^y \bmod n} \quad \xrightarrow{Y} \\
 K = X^y \bmod n \qquad K = Y^x \bmod n
 \end{array}
 \end{array} \right.
 \end{array}$$

$$\begin{array}{c}
 \left\{ \begin{array}{l}
 \text{PS} \\
 \begin{array}{c}
 \xrightarrow{PD = \text{dec}(K; PD_K)} \quad \xrightarrow{PD_K = \text{enc}(K; PD)} \\
 \xrightarrow{PD = \text{dec}(KM; PD_{KM})} \quad \xrightarrow{PD_{KM}}
 \end{array}
 \end{array} \right.
 \end{array}$$

Fig.